Claims:

1. A method for receiving a secure message pertaining to an electronic transaction conducted over an electronic network having a server and a portable electronic authorization device, comprising:

Receiving at said portable electronic authorization device first digital data, said first digital data representing said secure message; and

Searching for a share secret from a share secret table in said portable electronic authorization device;

If said share secret is found, decrypt said first digital data; otherwise compute said share secret in said portable electronic authorization device.

2. A method for transmitting a secure message pertaining to an electronic transaction conducted over an electronic network having a server and a portable electronic authorization device, comprising:

Searching for a share secret from a share secret table in said portable electronic authorization device;

If said share secret is found, encrypt first digital data; otherwise compute said share secret in said portable electronic authorization device.

Transmitting from said portable electronic authorization device said encrypted first digital data, said encrypted first digital data representing said secure message.

3. A method for receiving a secure message and approving the transaction pertaining to an electronic transaction conducted over a network having a server and a portable electronic authorization device, comprising:

Receiving at said portable electronic authorization device first digital data, said first digital data representing said secure message; and

Searching for a share secret from a share secret table in said portable electronic authorization device;

If said share secret is found, decrypt said first digital data; otherwise compute

said share secret in said portable electronic authorization device;

If a user approve said secure message, by pressing a button, generate a second digital data with a user information and a digital signature generated by said portable electronic authorization device;

Transmitting said second digital data to said electronic transaction system.

4. A method for transmitting a secure message and approving the transaction pertaining to an electronic transaction conducted over an electronic network having a server and a portable electronic authorization device, comprising:

If a user approve first digital data, by pressing a button, generate a digital data including a user information and a digital signature generated by said portable electronic authorization device;

Searching for a share secret from a share secret table in said portable electronic authorization device;

Transmitting at said portable electronic authorization device said encrypted second digital data, said encrypted second digital data representing said secure message.

5. A method of exchanging secured messages between first and second registered PEAD users over the internet and a server comprising the steps of obtaining public key information using the receiver's user ID as an index;

deriving a shared secret using the receiver's public key';

the sender then encrypting a message with the shared secret and sending it with the receiver's ID appended with the user's ID;

then the receiving PEAD user using the sender's user ID and sender's public key information to derive the shared secret.

6. A method is claimed in claim 5 including the step storing one or more of the other PEAD users' share secret using the sender's ID as an index.

7. A method is claimed in claim 5 wherein the sender retrieves the public key

information using the receiver's user ID from the server.

8. A method is claimed in claim 5 including the step of after the sender encrypts the message with the shared secret, sending it to the server with the receiver's ID appended.

9. A method is claimed in claim 4 including the further step of the server storing the sender's message, and thereafter forwarding the message to the receiver.

10. A method as claimed in claim 5 including the step of forwarding the message when the receiver's PEAD is polling for messages.

11. A method as claimed in claim 5 including the step of the server pushing the message to the receiver's PEAD.

12. A method as claimed in claim 5, including the step of the sender causing the PEAD to down load a key pair comprising a public key and a private key, and then transferring the public key to a server to be stored and indexed by the sender's ID.

13. A method as claimed in claim 6 including the step of the receiver checking for a stored shared secret in a shared secret table of the PEAD, and after finding the shares secret using the shared secret to decrypt the senders message.

14. A method as claimed in claim 13 wherein if the receiver does not find a shared secret in the shared secret table of the receiver's PEAD, then the receiver retrieves the senders public key information from the server using a sender's user ID as an index.

15. A method as claimed in claim 14 including the further step of the receiver using the receiver's private key and the now-retrieved sender's public key to compute the shared secret.

16. A method as claimed in claim 15 including the further of storing the shared secret, using the senders ID as an index.

17. A method as claimed in claim 16 including the further step of periodically updating the shared secrets stored in the shared secret table to reflect a change in a public key.